



# CVE-2020-14758

Published on: 10/21/2020 12:00:00 AM UTC

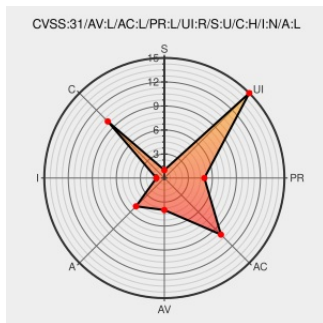
Last Modified on: 03/23/2021 11:24:00 PM UTC

## CVE-2020-14758

Source: Mitre

Source: Nist

Print: PDF



Certain versions of **Solaris** from **Oracle** contain the following vulnerability:

Vulnerability in the Oracle Solaris product of Oracle Systems (component: Kernel). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Solaris accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Solaris. CVSS 3.1 Base Score 5.6 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:L).

CVE-2020-14758 has been assigned by [secalert\\_us@oracle.com](mailto:secalert_us@oracle.com) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Oracle Corporation - Solaris Operating System** version = 11

CVSS3 Score: **5.6 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
<b>LOCAL</b>	<b>LOW</b>	<b>LOW</b>	<b>REQUIRED</b>
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
<b>UNCHANGED</b>	<b>HIGH</b>	<b>NONE</b>	<b>LOW</b>

CVSS2 Score: **3.6 - LOW**

Access Vector	Access Complexity	Authentication
<b>LOCAL</b>	<b>LOW</b>	<b>NONE</b>
Confidentiality Impact	Integrity Impact	Availability Impact

## CVE References

Description	Tags	Link
Oracle Critical Patch Update Advisory - October 2020	<a href="#">Patch</a> <a href="#">Vendor Advisory</a> <a href="#">www.oracle.com</a> <a href="#">text/html</a>	<a href="https://www.oracle.com/security-alerts/cpuoct2020.html">MISC www.oracle.com/security-alerts/cpuoct2020.html</a>

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Oracle	Solaris	11	All	All	All
Operating System	Oracle	Solaris	11	All	All	All
<input type="text" value="cpe:2.3:o:oracle:solaris:11.*.*.*.*.*.*"/>						
<input type="text" value="cpe:2.3:o:oracle:solaris:11.*.*.*.*.*.*"/>						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2021 [T](#) [N](#) |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)